UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT GREENEVILLE

UNITED STATES OF AMERICA	)	
	)	
v.	)	No. 2:19-CR-14
	)	District Judge Greer
XIAORONG YOU	)	
aka SHANNON YOU	)	

CERTIFICATE OF AUTHENTICITY PURSUANT TO FEDERAL RULE OF EVIDENCE 902(14)

I, [redacted] attest, under the penalty of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct.

a. I am a qualified person within the meaning of Federal Rule of Evidence 902(14) because I have performed forensic analysis of computers since 2015 as part of my job in the IT Security group at [redacted] I received a certification for completing Windows Forensic Analysis training provided by SANS (Systems Architecture Network & Security) Institute in 2015; that training covered the standard practices for creating and verifying forensic images of computers. Since 2015, I have continued to complete various trainings related to computer forensics and the creation of forensic images. Since 2015, I have created dozens of forensic images of computers as part of my job.

b. The original electronic device or storage medium at issue here is a 256 GB Micron M.2 drive (serial number UFZNP01ZR76JJ6) from an HP Elitebook Folio laptop (serial number 5CD7307M8J) belonging to [redacted] As a standard practice, [redacted] encrypts its electronic devices and storage media. I decrypted the original electronic device or storage medium before creating a forensic image. I copied the data contained on that decrypted device or medium to create the forensic image that was provided to the Federal Bureau of Investigation (FBI) on or about July 3, 2018.

c. I certify that the forensic image provided to the FBI is an exact duplicate of the accessible sectors for the decrypted original electronic device or storage medium.

d. I verified that the forensic image was an exact duplicate of the accessible sectors for the decrypted original electronic device or storage medium using the following process of

digital identification. The verification step in the forensic image acquisition process uses a mathematical algorithm which calculates a unique value based on the contents of the original data. This unique value is known as a "hash value" and can be thought of as a digital fingerprint which uniquely identifies the contents of the original device. A hash value is calculated for the contents of the original device and another hash value is calculated for the contents of the acquired forensic image. When the two hash values calculated are identical, this indicates the acquired forensic image is an exact duplicate of the accessible sectors from the original digital storage device.

[redacted]

5-27-2020
Date